Optical Review (2018) 25:540–548
https://doi.org/10.1007/s10043-018-0445-0

REGULAR PAPER

# One-time pad image encryption based on physical random numbers from chaotic laser

Jianzhong Zhang[1,2] · Changkun Feng[1,2] · Mingjiang Zhang[1,2] · Yi Liu[1,2]

Received: 25 January 2018 / Accepted: 30 June 2018 / Published online: 9 July 2018

**Abstract**
A one-time pad image encryption scheme based on physical random numbers from chaotic laser is proposed and explored. The experimentally generated physical random numbers serving as the encryption keys are constructed into two random sequence image matrices, which are applied to shuffle the pixel position of the original image and change its pixel value, respectively. Some tests including statistical analysis, sensitivity analysis, and key space analysis are performed to assess reliability and efficiency of the image encryption scheme. The experimental results show that the image encryption scheme has high security and good anti-attack performance.

**Keywords** Image encryption · Physical random number · Chaotic laser · One-time pad

## 1 Introduction

The popularization of the internet and cloud technology has given rise to the widespread transmission of digital images between network users. The security of the digital image information becomes increasingly important. Conventional encryption algorithms (i.e., DES, AES, and IDEA) are not appropriate for image encryption but for text data encryption, because the image has special characteristics such as large storage and high pixel correlation [1]. Therefore, a great many new and different image encryption schemes have been continuously put forward and explored.

At present, available image encryption schemes are mainly divided into two categories: chaos-based and non-chaos-based encryption algorithms. Chaos-based cryptosystems have been extensively investigated because chaos is characteristic of inner randomness and initial sensitivity. Moreover, a large amount of various chaotic maps have been proposed to encrypt the image with a permutation–diffusion structure, for example, Logistic map [2], Lorenz map [3], Tent map [4], Chen map [5], Jacobian elliptic map [6], Cat map [7], Hyper chaos [8], Laser chaos [9, 10], and the mixture of the above chaotic maps [11, 12]. Besides, many non-chaos-based encryption systems have been brought forward for the image encryption, for instance, block-based transformation algorithm [13], SCAN methodology [14], fractional Fourier transform (FRFT) [15], Rubik's Cube principle [16], DNA encoding algorithm [17], Quantum Hash function [18], and combinational permutation technique based on pseudorandom sequences [19].

According to Shannon's theory of secure communication [20], only the one-time pad cryptosystem is theoretically unbreakable. Moreover, the one-time pad key should be generated by true random number generator (TRNG), never be reused, and have the same length as the plain message. Therefore, the utilization of the true random number-based key may be the final solution to the image encryption. Recently, Liu et al. [21] has proposed that true random numbers from environmental noise serve as the one-time initial values of a chaotic system, and the image is finally encrypted by employing the sequences from the chaotic system to diffuse the pixels with the Exclusive OR (XOR) operation. T. Sivakumar et al. [22] have demonstrated that true random numbers from the noise audio signal are applied to XOR the

✉ Jianzhong Zhang
zhangjianzhong@tyut.edu.cn

✉ Mingjiang Zhang
zhangmingjiang@tyut.edu.cn

[1] Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, People's Republic of China

[2] Institute of Optoelectronic Engineering, College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, People's Republic of China

scrambled image, the pixel position of which is permuted by Knight's Travel Path. In general, the image encryption procedure mainly includes two steps, i.e., pixel permutation and diffusion. However, for the above image encryption schemes in [21, 22], the true random number is used as the encryption key only in the diffusion process to change the pixel values. To strengthen the security of the image encryption scheme, the true random number should be employed as the secret key in both the permutation and diffusion processes.

In this paper, the image encryption scheme based on physical random numbers from the chaotic laser system is proposed, where the physical random number sequences are constructed into the two random sequence image matrices to alter the pixel position in the permutation stage and change the pixel value in the diffusion phase.

## 2 Image encryption scheme

The schematic diagram of the image encryption based on physical random numbers extracted from the chaotic laser system is shown in Fig. 1. We refer to the transmitting end as Alice and the receiving end as Bob. The encrypted image messages can be transmitted on the internet by a set of protocols such as TCP/IP. In our scheme, we use the algorithm called one-time pad to encrypt the transmitted image, where the physical random numbers are utilized as the encryption key for both communication parties. In the encryption processes, a large number of the physical random numbers are first stored in the cloud by utilizing the advanced cloud technology [23]. Then, Alice and Bob download the same physical random numbers from the cloud on compact disks (CDs) or removable hard disks (HDs) with large capability storage. The common encryption key is extracted from the downloaded physical random number pool. The extraction approach of the secret key can function as the private key, which could be exchanged by means of quantum key distribution protocol [24] and the semiconductor lasers' synchronization by injecting common light [25]. The image encryption/decryption process consisting of two distinct stages, namely permutation and diffusion, is depicted in the block diagram of Fig. 1. In the permutation phase (D), the pixel positions of the original image are completely randomly permutated and in the diffusion phase (F), the statistical pixel values are changed. The concrete encryption/decryption procedures are given below.

## 3 Generation of random sequences

### 3.1 Experimental setup

The physical random number generation has been experimentally achieved using a chaotic laser as physical entropy source [26, 27]. Figure 2 shows our experimental setup of physical random number generation. The chaotic light source consists of a distributed-feedback (DFB) laser diode, a fiber coupler, a polarization controller (PC), a variable optical attenuator (VOA), and a fiber mirror (FM). More details are available in [27]. When the chaotic light source operates under the following parameters: the operating current is set to 1.5 times its threshold current (22 mA), the feedback strength is 30% of the laser output power, and the external cavity length is about 8.4 m, it generates chaotic

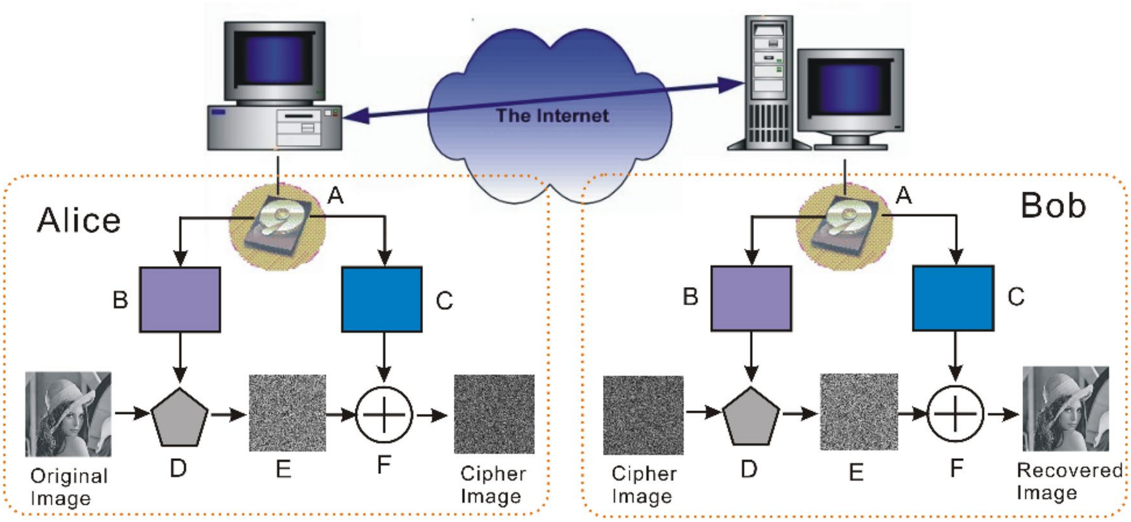


**Fig. 1** The image encryption scheme based on physical random numbers from chaotic laser system. Symbols: *A* physical random number pool, *B* the constructed random sequence image $\mathrm{RSI}_{M,N^1}$, *C* the constructed random sequence image $\mathrm{RSI}_{M,N^2}$, *D* permutation operation in encryption, *E* the shuffled image, and *F* XOR operation in encryption

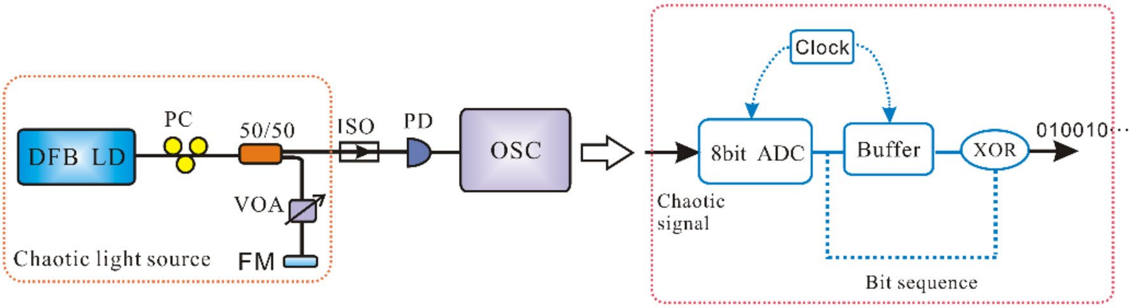


**Fig. 2** Experimental setup of physical random number generation

signals with high frequency. The output chaotic light through an optical isolator (ISO) is converted to electrical signals by a photodetector (PD). The ISO ensures that the chaotic light has a one-way transmission direction. The detected chaotic signal is sampled by the 8-bit analog-to-digital (ADC) of an oscilloscope (OSC). The binary sequence is off-line obtained through the following procedure. A single 8-bit digital signal is first down-sampled to the lower sampling rate by the Clock. By XOR operating the corresponding pairs of bits in the 8-bit digital signal and its bit-delayed one stored in the Buffer, the single down-sampled 8-bit digital signal is further given. Finally from each sample, the least significant bits (LSBs) are selected and interleaved to achieve a binary sequence.

### 3.2 Statistical properties of random sequence

Afterward, we analyze the statistical properties of the generated random sequence. Figure 3a displays the waveform of the chaotic signal acquired by the oscilloscope with the set sampling rates of 20 GS/s. To decrease the correlation of the adjacent samples, an external down-sampling to 2 GS/s is utilized, that is, one out of each ten samples is extracted. The randomness of the single random binary sequence is evaluated using the NIST test suite [28]. The test results show that for the constructed sequence by employing only one of the 8 bits at each sample, the first to seventh LSB can pass statistical tests of randomness but the most significant bit cannot. The reason why the most significant bit cannot pass the NIST test has been analyzed in detail in [29]. So, seven LSBs from each sample are adopted as a subset to construct a single bit sequence. The obtained random bit sequence is further tested and passes all of the NIST tests. The typical results are given in Fig. 4. Pass criteria are determined by the sequence length and the significance level. A significance level $\alpha = 0.01$ is set for $P$ value of each sequence test. For the 1000 samples of 1 Mb data, the proportion of sequences that satisfy $P$ value $> \alpha$ is estimated to be $0.99 \pm 0.0094392$. Figure 3b depicts the autocorrelation trace of the obtained random sequence with characteristic of δ-like function. This means that the knowledge of the random bits for some given time does not predict the future evolution of the random sequence. Thus, the extracted random binary bit sequence can be applied to the encryption of the image.

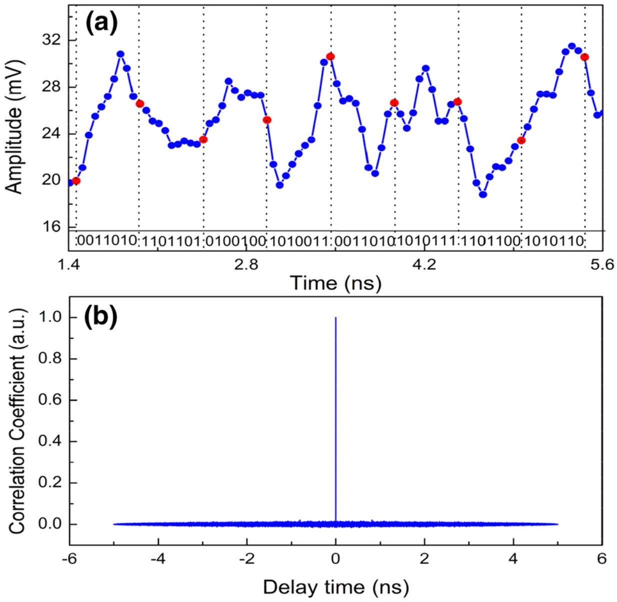


**Fig. 3** **a** The extracted random sequence from chaotic signal and **b** autocorrelation trace of the extracted random sequence

## 4 Image encryption procedure

### 4.1 Preprocessing stages

1. Under normal circumstances, a gray digital image P is composed of a two-dimensional matrix, which contains integers ranging from 0 to 255. However, as is mentioned before, the key shared by Alice and Bob is an infinitely long binary sequence, $B_i = \{b_1, b_2, \ldots, b_\infty\}$, where $b_\text{i} = 0$ or 1. To further realize the image cryptography, we need to preprocess the binary sequence. Here,

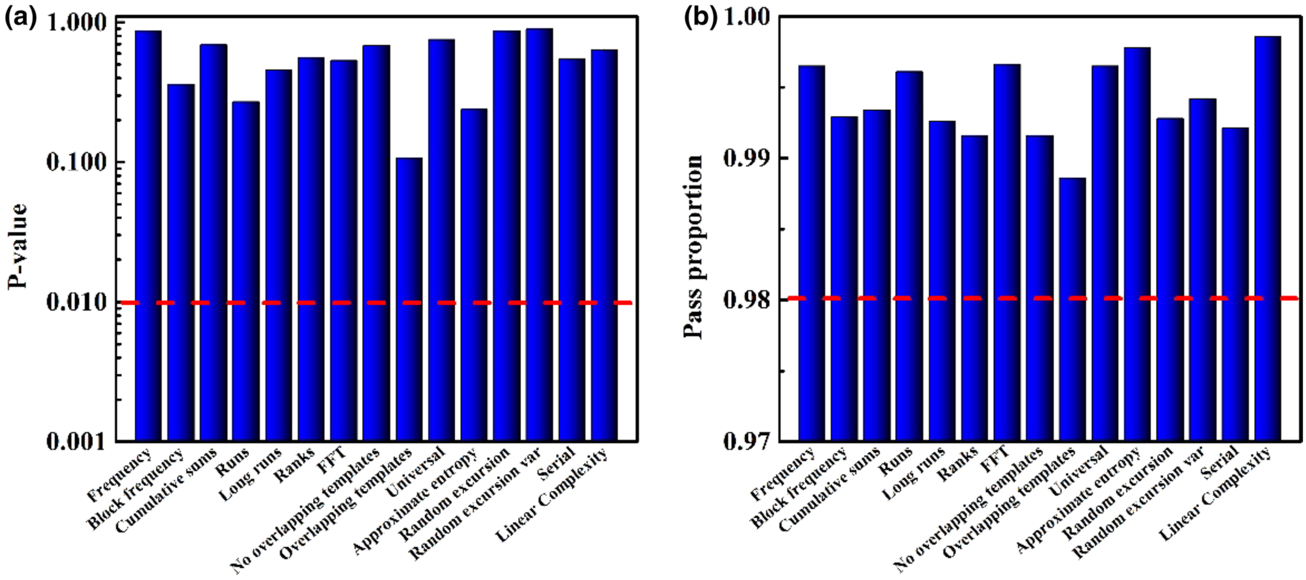


**Fig. 4** Results of NIST statistical tests. All tests are passed using 1000 samples of 1-Mb data at the significance level of $\alpha = 0.01$ and with the proportion within the range of $0.99 \pm 0.0094392$

a double encryption method is employed in the proposed image encryption scheme. During the image encryption process, the two sets of different keys, namely $K^1 = \{k_1{}^1, k_2{}^1, \ldots, k_\infty{}^1\}$and$K^2 = \{k_1{}^2, k_2{}^2, \ldots, k_\infty{}^2\}$, are constructed according to the following equation:

$$\begin{aligned} k_i^{1,2} = {} & b_{i\times 8+1} \times 2^0 + b_{i\times 8+2} \times 2^1 + b_{i\times 8+3} \times 2^2 \\ & + b_{i\times 8+4} \times 2^3 + b_{i\times 8+5} \times 2^4 \\ & + b_{i\times 8+6} \times 2^5 + b_{i\times 8+7}{}^1 \times 2^6 + b_{i\times 8+8}{}^1 \times 2^7, \end{aligned} \tag{1}$$

where i = 1, 2, ..., $\mathrm{k_i}^{1,2} \in [0, 255]$.

2. Next, a subset of integers from the data set $K^1$ and $K^2$ is selected and further processed into $K^{1'}$ and $K^{2'}$, respectively, which are two arrays of $M \times N$ data elements with $M$ rows and $N$ columns. The concrete processing rules are given as follows:

$$K^{1'} \leftarrow \mathrm{reshape}(K^1, M, N) \tag{2}$$

$$K^{2'} \leftarrow \mathrm{reshape}(K^2, M, N), \tag{3}$$

where reshape means to change the size of $K^1$ and $K^2$ to $M \times N$ array. The result of this operation will obtain two arrays, $K^{1'}$ and $K^{2'}$, containing a $M \times N$ number of elements. $K^{1'}$ and $K^{2'}$ can be also represented as two image matrices labeled as the Random Sequence Image $\mathrm{RSI}_{M,N^1}$ and $\mathrm{RSI}_{M,N^2}$, which correspond to B and C in Fig. 1, respectively. Here, they will serve as the permutation mask in the permutation phase and the substitution mask in the diffusion stage.

## 4.2 Image position shuffling

The plain image data have strong correlations between the adjacent pixels. To eliminate the high pixel correlation, $\mathrm{RSI}_{M,N^1}$ is utilized to shuffle the position of the original image in the permutation stage. The procedure of shuffling image is described as follows:

1. The elements of $\mathrm{RSI}_{M,N^1}$ are sorted in ascending order according to their pixel values. The $\mathrm{RSI}_{M,N^1}$ is transformed into a new image matrix known as $\mathrm{RSI}_{M,N^{1'}}$. Each element of the $\mathrm{RSI}_{M,N^{1'}}$ constitutes the indices for position shuffling of the original image P.
2. All the $M$ columns and $N$ rows of P with $\mathrm{RSI}_{M,N^{1'}}$ are shuffled into the intermediate transformation matrix E (shown in Fig. 1).

## 4.3 Image statistics change

In the diffusion stage, the image matrix $\mathrm{RSI}_{M,N^2}$ derived from Eq. (3) is utilized to alter the statistical information of the intermediate transformation image E through the XOR operation. The symbol $\oplus$ represents the bit-by-bit XOR operation. Thus, the cipher image $\mathrm{P^c}$ is obtained according to the following formula:

$$P^c \leftarrow E \oplus \mathrm{RSI}_{M,N^2}. \tag{4}$$

The decryption procedure is similarly performed in terms of the encryption one listed above. The same key sets $K^1$ and $K^2$ at the receiving end are first achieved as indicated in preprocessing stages. Then, we carry out the anti-XOR and reverse permutation operation to correctly recover the original image P.

## 5 Security analysis

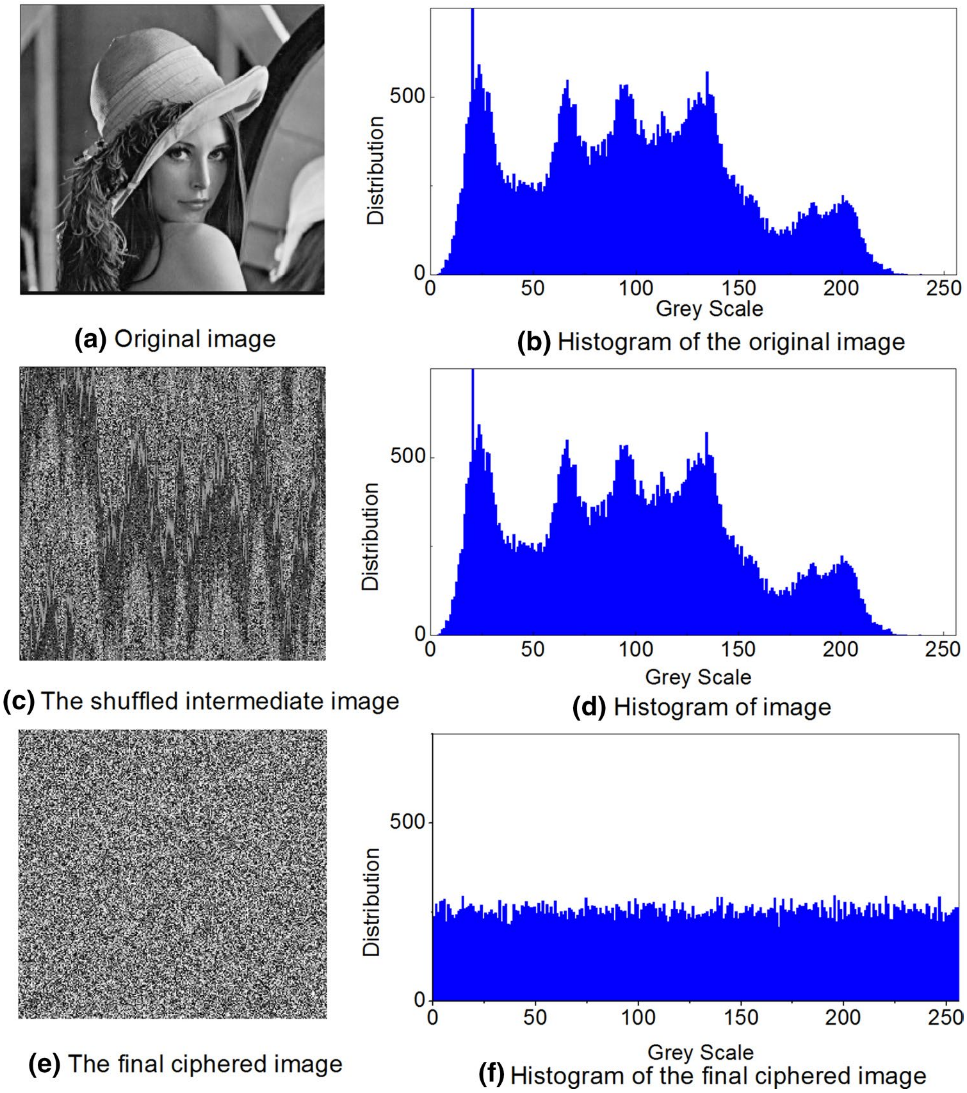
It is well known that a high-equality encryption algorithm should resist all kinds of brute force attacks, such as cryptanalytic and statistical attacks. Here, we examine the security of the proposed image encryption scheme by utilizing this scheme to encrypt a Lena BMP image with the size 256 × 256 shown in Fig. 5a. Some security tests including statistical analysis, sensitivity analysis, and key space analysis on our image encryption scheme have been performed in the following.

### 5.1 Statistical analysis

In fact, many cryptographic algorithms have been successfully cracked by employing the statistical analysis. Here, to further demonstrate the robustness of our image encryption procedure, we have carried out statistical analysis by calculating the histograms of the encrypted images and the correlations of two adjacent pixels.

#### 5.1.1 Histogram analysis

Figure 5a, c, e presents the plain image of Lena, the shuffled intermediate image, and the final ciphered image, respectively. Their corresponding computed gray-scale histograms are depicted in Fig. 5b, d, f. From the statistical information



**(a)** Original image

**(b)** Histogram of the original image

**(c)** The shuffled intermediate image

**(d)** Histogram of image

**(e)** The final ciphered image

**(f)** Histogram of the final ciphered image

**Fig. 5** Histograms of the images

depicted in Fig. 5d, we can see that the shuffled image has the same statistical histograms as the original image although it does not display portrait information of Lena. From the viewpoint of statistical attack, it is not safe. Thus, the XOR operation on the shuffled image in the diffusion phase is necessary to further alter the statistical information. Figure 5f clearly shows that the histogram of the finally encrypted image is fairly uniform and distinctly different from the histogram of the plain image. We further quantitatively compare the statistics of the plain and ciphered images. The average value and standard deviation of the plain image are 97.772 and 52.778, respectively. The average value and standard deviation of the ciphered image are 127.451 and 74.064, respectively. Moreover, the statistics of the other plain and ciphered images obtained by our image encryption algorithm are quantitatively tested as well. The results demonstrate that the average values and standard deviations of all the ciphered images are approximately 127 and 74, respectively, no matter what the gray-scale distribution of the original image is. Therefore, any clue cannot be provided from the altered statistical histograms to perform any statistical attack on our image encryption scheme.

#### 5.1.2 Correlation analysis

Apart from the histogram analysis, the correlations between two adjacent pixels in the plain image and its encrypted image are analyzed as well. First, 1000 pairs of two adjacent pixels are randomly selected along horizontal, vertical, and diagonal directions from an image, respectively. Then, the correlation coefficient of each pair is calculated according to the following formulas [7]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{5}$$

where $x$ and $y$ are gray-scale values of two adjacent pixels in the image, respectively, and $N = 1000$ is total number of pixels. Figure 6 illustrates the correlation distribution of two adjacent pixels along the horizontal, vertical and diagonal directions in the plain and ciphered images. The corresponding correlation coefficients are shown in Table 1. From Fig. 6 and Table 1, we can see that the correlation between the two adjacent pixels in the encrypted image is negligible although it is high in the plain image. So, our image encryption scheme meets a strict criterion that the correlation values of adjacent pixels should be minimal for the encrypted image.

### 5.2 Sensitivity analysis

In this section, the sensitivity analysis of our image encryption scheme is further performed. We analyze the image decryption effect for the various extraction methods of the secret key. As is mentioned before, the secret keys for the image encryption and decryption are generated by utilizing Eq. (1). Figure 7a illustrates the decrypted image when the decryption key extracted from the random number sequence has only a delay bit with the encryption key. The result shows that the plain image cannot be correctly retrieved. Only when the decryption process is completely consistent with the encryption one can the encryption system get the correct decrypted image, as illustrated in Fig. 7b.

### 5.3 Key space analysis

In general, a secure image encryption system should have a large enough key space to ensure that the brute force attack is infeasible. The presented image encryption scheme belongs to one-time pad system. The random numbers generated by chaotic laser system are used as the secret key to encrypt the plain image. Thus, an image cipher has a very large key space of size $2^{M\times N}$, which is determined by the size of the plain image. As is mentioned before, an image with the size of 256 × 256 is chosen and the corresponding key space size is $2^{256\times 256}$. This pretty exhaustive key space makes our system resistant to brute force attack. Actually, the multiple initial values of chaotic laser system and many key extraction methods from long enough random number sequence ensure that the attackers cannot do anything about our image encryption system.

### 5.4 Resistance to attacks

At present, there are four classical types of attacks based on the level of knowledge of the attackers to the cryptosystem, which are enumerated from the hardest to the easiest: ciphertext only, known plaintext, chosen plaintext, and chosen ciphertext. According to Kerchoff's principle, cryptanalyst knows everything about the cryptosystem except the secret key. Therefore, the chaos-based or non-chaos-based image encryption algorithms have a theoretical possibility of cracking when the above four types of attacks are utilized. However, our image encryption scheme adopting one-time pad encryption method is explored, which is theoretically

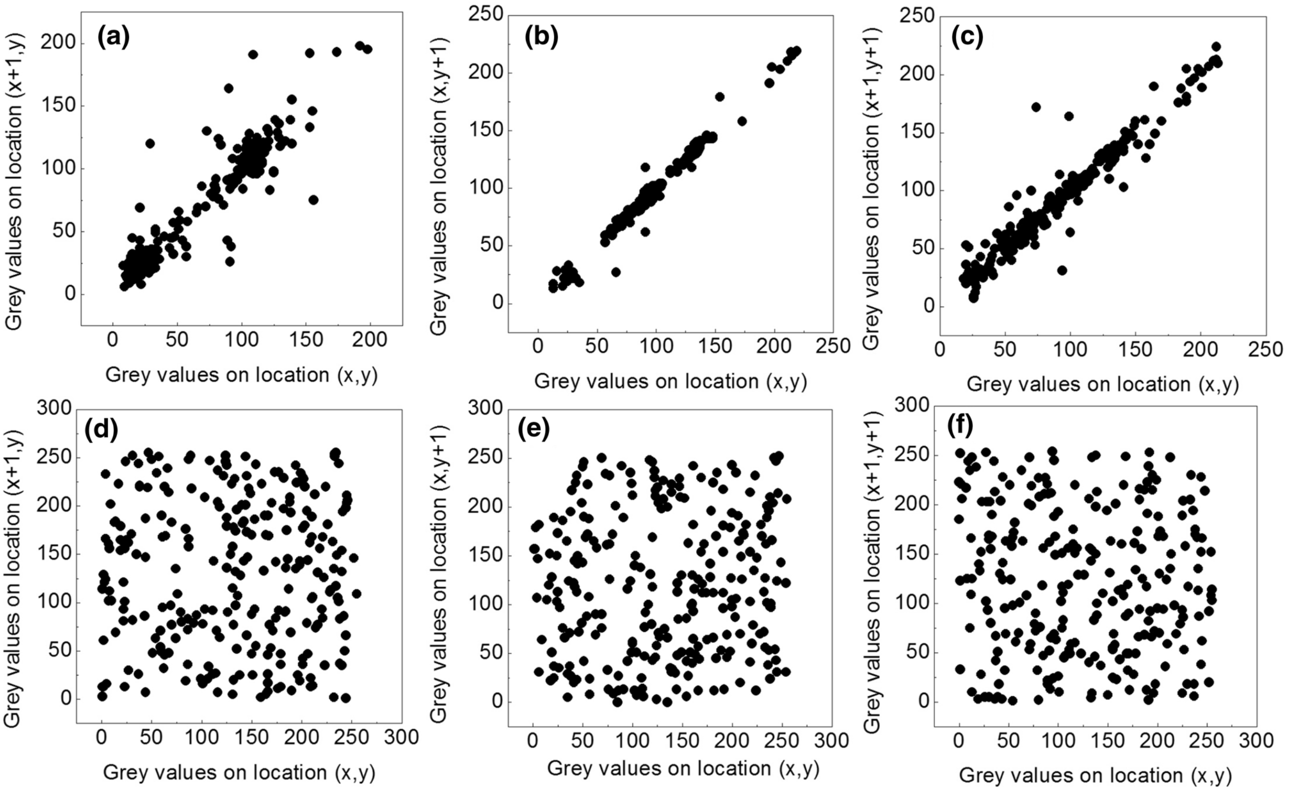


**Fig. 6** Correlations of two adjacent pixels in the original image (upper row) and the encrypted image (lower row). **a, d** Horizontal direction. **b, e** Vertical direction. **c, f** Diagonal direction

**Table 1** Correlation coefficients of two adjacent pixels in the original and encrypted images

| | Original image | Encrypted image |
|---|---|---|
| Horizontal | 0.9747 | 0.0515 |
| Vertical | 0.9716 | 0.0316 |
| Diagonal | 0.9518 | 0.0249 |

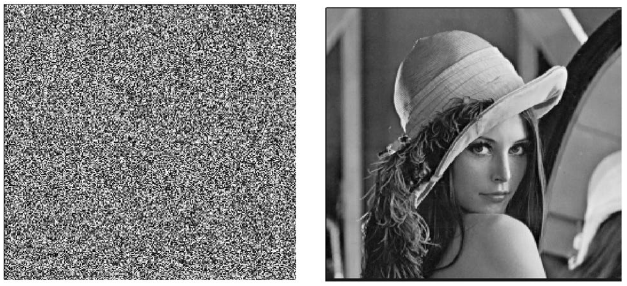

**(a)** incorrect decrypted key **(b)** correct decrypted key

**Fig. 7** Sensitivity test. **a** The decrypted image using the decrypted key having a delay bit with the encrypted key. **b** The decrypted image with correct key

unbreakable in term of Shannon's theory. So, our image encryption scheme may resist these four types of attacks.

## 5.5 Speed analysis

For a good image encryption algorithm, the computational complexity is also an important aspect. As is illustrated above, the proposed image encryption scheme mainly consists of two parts: the generation of true random numbers as one-time pad key and the image encryption/decryption procedure. The security of our image encryption scheme relies not on the encryption algorithm itself but on the secret key. Therefore, the image encryption/decryption procedure is extremely simple. The physical random number sequences from chaotic laser entropy source are constructed into two random sequence image matrices to alter the pixel position in the permutation stage and change the pixel value in the diffusion phase, respectively. The average encryption/decryption time is 0.017 s on a gray-scale image of the size 256×256. The time analysis has been done on personnel computer with clock speed of 3.60 GHz and 8 GB of RAM memory.

## 6 Discussion

Compared with the proposed scheme in [21], our image encryption scheme has two obvious advantages, although both encryption schemes are based on physical random numbers. On the one hand, in our proposed scheme, the chaotic laser is utilized as an entropy source to extract physical random numbers. Compared with the environment noise, the chaotic laser has higher spectral density and in the same bandwidth has higher output power, which is more prone to generate high-quality physical random numbers. The generated random numbers pass the NIST test. On the other hand, our scheme explores one-time pad encryption method to achieve the image encryption, where the physical random numbers are directly constructed into two random sequence image matrices to shuffle the pixel position of the original image and change its pixel value, respectively. However, for the proposed scheme in [21], the physical random numbers are served as the one-time initial values of a chaotic system, and the image is finally encrypted by employing the sequences from the chaotic system to diffuse the pixels with the XOR operation. Therefore, compared with the key space ($10^{59}$) of the proposed scheme in [21], our scheme has larger key space with the size of $2^{256\times256}\approx10^{183}$, which ensures higher security of our image encryption scheme. Besides, the security of our scheme only depends on the secret key whereas the security of the proposed scheme in [21] is related to not only the secret key itself but also the encryption algorithm. Thus, our scheme provides simpler image encryption means and shorter measurement time when the encrypted image sizes are same.

## 7 Conclusions

In conclusion, a novel one-time pad image encryption scheme based on physical random numbers from chaotic laser system is proposed and verified. The statistical properties of the experimentally generated physical random numbers serving as the secret keys are analyzed and tested. The image encryption/decryption procedures are given in detail. Some tests such as statistical analysis, sensitivity analysis, and key space analysis demonstrate that the proposed image encryption scheme has superior performance compared with many existing image encryption algorithms, such as the theoretically absolute security, the good statistical property, and the high sensitivity. So, our encryption scheme will show potential application prospect in the field of image encryption.

**Acknowledgements** This work is supported by the National Natural Science Foundation of China (NSFC) under Grant 61527819, by Research Project Supported by Shanxi Scholarship Council of China under Grant 2016-036 and 2017-052, and by Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi and Program for Sanjin Scholar.

## References

1. Zhu, C.X.: A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun. **285**, 29–37 (2012)
2. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image Vis. Comput. **24**, 926–934 (2006)
3. Arroyo, D., Li, C.Q., Li, S.J., Alvarez, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos Solitons Fractals **41**, 2613–2616 (2009)
4. Ghebleh, M., Kanso, A.: A novel efficient image encryption scheme based on chained skew tent maps. Neural Comput. Appl. **28**, 953–967 (2017)
5. Guan, Z.H., Huang, F.J., Guan, W.J.: Chaos-based image encryption algorithm. Phys. Lett. A **346**, 153–157 (2005)
6. Behnia, S., Akhavan, A., Akhshani, A., Samaudin, A.: Image encryption based on the Jacobian elliptic maps. J. Syst. Softw. **86**, 2429–2438 (2013)
7. Chen, G.R., Mao, Y.B., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **21**, 749–761 (2004)
8. Gao, T.G., Chen, Z.Q.: A new image encryption algorithm based on hyper-chaos. Phys. Lett. A **372**, 394–400 (2008)
9. Banerjee, S., Rondoni, L., Mukhopadhyay, S., Misra, A.P.: Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption. Opt. Commun. **284**, 2278–2291 (2011)
10. Wang, S.Y., Zhao, J.F., Li, X.F., Zhang, L.T.: Image blocking encryption algorithm based on laser chaos synchronization. J. Electr. Comput. Eng. https://doi.org/10.1155/2016/4138654 (2016)
11. Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**, 408–419 (2008)
12. Alsafasfeh, Q.H., Arfoa, A.A.: Image encryption based on the general approach for multiple chaotic systems. J. Signal Inf. Process. **2**, 238–244 (2011)
13. Younes, M.A.B., Jantan, A.: Image encryption using block-based transformation algorithm. IAENG Int. J. Comput. Sci. **35**, 407–415 (2008)
14. Maniccam, S.S., Bourbakis, N.G.: Image and video encryption using SCAN patterns. Pattern Recognit. **37**, 725–737 (2004)
15. Tao, R., Meng, X.Y., Wang, Y.: Image encryption with multiorders of fractional Fourier transforms. IEEE Trans. Inf. Forensics Sect. **5**, 734–738 (2010)
16. Loukhaoukha, K., Chouinard, J.Y., Berdai, A.: A secure image encryption algorithm based on Rubik's cube principle. J. Electr. Comput. Eng. https://doi.org/10.1155/2013/848392 (2012)
17. Akhavan, A., Samsudin, A., Akhshani, A.: Cryptanalysis of an image encryption algorithm based on DNA encoding. Opt. Laser Technol. **95**, 94–99 (2017)
18. Yang, Y.G., Xu, P., Yang, R., Zhou, Y.H., Shi, W.M.: Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. Sci. Rep. **6**, 19788 (2016)
19. Mitra, A., Rao, Y.V.S., Prasanna, S.R.M.: A new image encryption approach using combinational permutation techniques. World Acad. Sci. Eng. Technol. **14**, 919–923 (2008)
20. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)

21. Liu, H.J., Kadir, A., Sun, X.B.: Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. IET Image Process. **11**, 324–332 (2017)
22. Sivakumar, T., Venkatesan, R.: A new image encryption method based on Knight's travel path and true random number. J. Inf. Sci. Eng. **32**, 133–152 (2016)
23. Random number download website. http://random-number.net. Accessed 4 May 2018
24. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441–444 (2000)
25. Yoshimura, K., Muramatsu, J., Davis, P., Harayama, T., Okumura, H., Morikatsu, S., Aida, H., Uchida, A.: Secure key distribution using correlated randomness in lasers driven by common random light. Phys. Rev. Lett. **108**, 070602 (2012)
26. Kanter, I., Aviad, Y., Reidler, I., Cohen, E., Rosenbluh, M.: An optical ultrafast random bit generator. Nat. Photonics **4**, 58–61 (2010)
27. Zhang, J.Z., Wang, Y.C., Liu, M., Xue, L.G., Li, P., Wang, A.B., Zhang, M.J.: A robust random number generator based on differential comparison of chaotic laser signals. Opt. Express **20**, 7496–7506 (2012)
28. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. Accessed 4 May 2018
29. Argyris, A., Deligiannidis, S., Pikasis, E., Bogris, A., Syvridis, D.: Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit. Opt. Express **18**, 18763–187638 (2010)